



## A Process for Managing Risks in Distributed Teams

Persson, John Stouby; Mathiassen, Lars

*Published in:*  
IEEE Software

*DOI (link to publication from Publisher):*  
[10.1109/MS.2009.157](https://doi.org/10.1109/MS.2009.157)

*Publication date:*  
2010

*Document Version*  
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

*Citation for published version (APA):*  
Persson, J. S., & Mathiassen, L. (2010). A Process for Managing Risks in Distributed Teams. *IEEE Software*, 27(1), 20-29. <https://doi.org/10.1109/MS.2009.157>

### General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

### Take down policy

If you believe that this document breaches copyright please contact us at [vbn@aub.aau.dk](mailto:vbn@aub.aau.dk) providing details, and we will remove access to the work immediately and investigate your claim.

## A Process for Managing Risks in Distributed Teams

**John Stouby Persson**, Aalborg University

**Lars Mathiassen**, Georgia State University

A process for managing risks associated with distributed software projects offers a series of rigorous but easy-to-follow steps.

**T**oday, many software projects are geographically distributed, so software managers must know how to manage distributed teams.<sup>1,2</sup> For example, they need to know how to build teams across sites, how to break down and distribute tasks, how to share knowledge across time, space, and cultural differences, and how to coordinate work to produce coherent outcomes.

The current literature offers rich insights into these challenges,<sup>2–5</sup> but it offers no process for managing risks that apply to distributed team structures. We've developed a comprehensive process that's compliant with CMMI, the Software Engineering Institute's maturity model for assessing and improving organizational processes. CMMI offers a comprehensive set of generic processes to support development of products and services.<sup>6</sup> One of its processes focuses on risk management to help identify and analyze potential problems before they occur so that managers can plan risk-handling activities and invoke them across the project life cycle. We adapt this approach to avoid redundancies and focus on managing risk in distributed teams. We describe a series of steps that are easy to understand and follow. However, practicing risk management requires nontrivial skills and insights,<sup>7</sup> so it's important to remember that a rigorous recipe for action must always be adapted to become useful in practice:

*A recipe tells you the ingredients, how to mix the ingredients, what temperature to use, and*

*how long to cook those ingredients. However, it does not teach you the techniques of slicing and dicing, mixing, beating, whipping, blanching, grilling, poaching, etc. And recipes also leave room for some experimentation and modification.<sup>8</sup>*

### Process Foundation

To create a solid foundation for the process, we synthesized state-of-the-art research on managing distributed teams.<sup>5</sup> Analyzing 72 scientific articles, we identified inherent risks in distributed teams, techniques to solve them, and guidelines for applying the techniques. We then integrated these findings into a framework to support risk management in distributed teams; a Web-based tool implementation of the framework is freely available at [www.distributedprojects.net](http://www.distributedprojects.net).

We synthesized the risks into a two-level taxonomy. First, we identified eight risk areas:<sup>5</sup>

- task distribution,
- knowledge management,
- geographical distribution,

- collaboration structure,
- cultural distribution,
- stakeholder relations,
- communication infrastructure, and
- technology setup.

Then, we identified specific risk factors to further characterize each risk area.<sup>7</sup> Table 1 defines risk areas and factors that are characteristic for distributed teams. Some of these might seem typical for any project, but the table focuses on risks related to distributed teams. Distributed environments can significantly intensify risks, to an extent that traditional project management approaches might not apply.

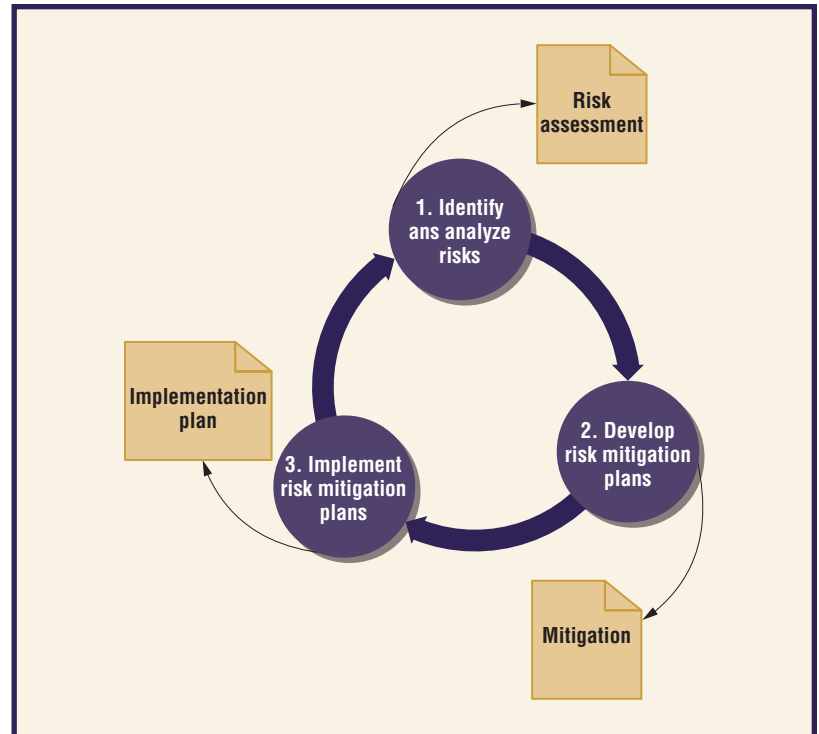
For example, the collaboration structure risk area includes a risk factor for collaboration capability (see Table 1).<sup>6,10,15</sup> This factor describes team members' understanding and appreciation of competency differences and how effectively they use technology to gather and share information over geographical and functional distances.<sup>5,9</sup> It's problematic if distributed team members have limited understanding of each other's competencies—for example, when a distributed team needs to manage software requirements across sites.<sup>8,10–11</sup>

Language barriers are another risk factor.<sup>6,10,15</sup> They arise when distributed team members don't share the same language or communication norms. Such situations can easily lead to misinterpretations and un conveyed information,<sup>5</sup> which are well-known problems in distributed teams.<sup>2–4,9</sup>

We also synthesized four different types of resolution techniques: planning, control, social integration, and technical integration:<sup>12</sup>

- *planning techniques* help design and organize projects so that they can be effectively executed in distributed contexts;
- *control techniques* facilitate tracking progress across sites and help manage discrepancies in relation to plans;
- *social integration techniques* integrate team members and help manage cultural differences across sites; and
- *technical integration techniques* increase connectivity and technical compatibility across sites.

Finally, we identified a portfolio of specific techniques for each type and guidelines for how to apply them to distributed-team risks (see Table 2). So, the eight areas of risks, the four types of resolution techniques, and the guidelines for combining them are syntheses of state-of-the-art research on distrib-



**Figure 1. Steps and outcomes in the risk management process. Circles are process steps and rectangles are outcomes. The first step addresses CMMI's second specific goal for risk management. The second and third steps address CMMI's third specific goal for risk management.**

uted teams and form the conceptual foundation for our risk management process.

## Process Architecture

We structured the risk management process into the three steps shown in Figure 1: identify and analyze risks, develop risk mitigation plans, and implement risk mitigation plans. We adopted a risk-action list approach in the risk management processes that offers directions for how to apply the four types of resolution techniques to the eight areas of distributed-team risks.<sup>13</sup> Managers of distributed teams can adopt our process when preparing for risk management, which is CMMI's first specific goal for risk management. Because the focus is on risks related to or exacerbated by project distribution, managers must adopt other processes for complete risk management when addressing CMMI's first specific goal.

The first process step in Figure 1 helps distributed team managers identify and analyze risks—CMMI's second specific goal for risk management.<sup>6</sup> We have identified and categorized the risks (see Table 1), so risk management participants can focus on analyzing risk probabilities and impacts and prioritize how to address them. It's particularly important to involve team members during this step because the project manager might have limited knowledge about different sites. For a given project, the first level of analysis therefore focuses on developing risk assessments at each site. The sec-

**Table 1****Identifying and analyzing distributed-team risks**

<b>Risk area</b>	<b>Risk factor and risk question</b>	<b>Low risk</b>	<b>Medium risk</b>	<b>High risk</b>
Task distribution	<i>Task uncertainty.</i> Do team members possess the knowledge and capabilities needed?	Team members know the task, and it fits well with their capabilities.	Team members have reasonable task knowledge, and their capabilities cover most challenges.	There are serious gaps in team members' task knowledge and required capabilities.
	<i>Task equivocality.</i> Do team members understand the specification of the task?	The task is well specified and understood by team members.	Most aspects of the specification are clear, and key team members understand the task.	The specification lacks clarity on major points, and many team members have limited task understanding.
	<i>Task coupling.</i> Is the task divided into distinct subtasks across sites?	There is minor need to coordinate development work across sites.	There is some need to coordinate development work across sites.	There is major need to coordinate development work across sites.
Knowledge management	<i>Knowledge creation.</i> How is task knowledge created across sites?	All sites contribute well to the creation of required task knowledge.	Most sites contribute reasonably well to the creation of required task knowledge.	There are major problems related to the creation of required task knowledge.
	<i>Knowledge capture.</i> How is task knowledge captured across sites?	Task knowledge is captured effectively across sites.	Task knowledge is, with some exceptions, captured effectively across sites.	There are major problems related to capturing task knowledge across sites.
	<i>Knowledge integration.</i> How is task knowledge integrated and shared across sites?	Task knowledge is integrated and shared well across sites.	Task knowledge is, with some exceptions, well integrated and shared across sites.	There is limited task knowledge integration and sharing across sites.
Geographical distribution	<i>Spatial distribution.</i> How many sites are involved, and what's the distance between them?	There are few sites collaborating over limited distance.	There are several sites collaborating over some distance.	There are many sites collaborating over considerable distance.
	<i>Temporal distribution.</i> How do time zone differences impact development work?	Time zone differences cause no or only minor problems.	Time zone differences require some ad hoc coordination across sites.	Time zone differences cause major problems and require constant attention across sites.
	<i>Goal distribution.</i> How diverse are goals across sites?	Team members share major goals across sites.	There is some variation in goals across sites.	There are major goal conflicts across sites.
Collaboration structure	<i>Collaboration capability.</i> Can team members collaborate across sites?	Team members collaborate across sites as needed.	In most cases, team members collaborate across sites as needed.	Breakdowns in collaboration across sites are common.
	<i>Coordination mechanisms.</i> Are coordination mechanisms appropriate across sites?	Coordination mechanisms are shared across sites and well adapted to the distributed context.	Coordination mechanisms are shared by most team members and reasonably well adapted to the distributed context.	Coordination mechanisms are not shared across sites and poorly adapted to the distributed context.
	<i>Process alignment.</i> Are processes aligned across sites?	Processes (including methods, templates, and guidelines) are shared across sites.	Processes (including methods, templates, and guidelines) vary but are reasonably well aligned across sites.	Processes (including methods, templates, and guidelines) are different across sites.
Cultural distribution	<i>Language barriers.</i> Do language and communication norms vary across sites?	Team members share language and communication norms across sites.	Team members use a common language with minor differences in communication norms.	Team members don't share a common language and have different communication norms.
	<i>Work culture.</i> Does work culture differ between sites?	Team members share work culture (including authority and team behavior) across sites.	Team members understand variations in work culture (including authority and team behavior) across sites.	Team members don't understand variations in work culture (including authority and team behavior) across sites.
	<i>Cultural bias.</i> Does cultural bias impact communication and cooperation across sites?	There are no major variations in cultural values across sites.	Team members communicate and collaborate based on appreciation of cultural variations across sites.	Team members lack knowledge of variations in cultural values across sites.

**Table 1 cont'd**

**Identifying and analyzing distributed-team risks**

Risk area	Risk factor and risk question	Low risk	Medium risk	High risk
Stakeholder relations	<i>Stakeholder commitment.</i> Are stakeholders committed to the project?	Key stakeholders are committed and share a common project identity across sites.	Most stakeholders are committed to the project and know about its distributed organization.	Stakeholder commitment varies, and there is no shared project identity.
	<i>Mutual trust.</i> Is there trust between stakeholders across sites?	There is appropriate mutual trust across sites.	There are instances of insufficient trust across sites.	Stakeholders don't trust each other across sites.
	<i>Relationship building.</i> Can the project integrate stakeholders across sites?	Existing and new stakeholders are well integrated across sites.	Existing and new stakeholders are mostly integrated well across sites.	There are several cases of stakeholders not being well integrated.
Communication infrastructure	<i>Personal communication.</i> What's the level of personal communication and social interaction across sites?	The level of personal communication and social interaction across sites is appropriate.	There is some personal communication and social interaction across sites.	There is limited personal communication and social interaction across sites.
	<i>Interaction media.</i> How well is communication across sites supported by media?	Communication needs across sites are well supported by media.	Communication across sites is for many purposes well supported by media.	There are severe shortcomings in media support of communication across sites.
	<i>Teleconference management.</i> How well is teleconferencing managed across sites?	Teleconferencing is used appropriately and managed effectively across sites.	Teleconferencing is used to some extent across sites and reasonably well managed.	There is limited use of teleconferencing across sites and they aren't managed well.
Technology setup	<i>Network capability.</i> Are communication networks reliable?	Networks aren't causing delays in development work and communication.	Networks are causing some delays in development work and communication.	Networks are causing serious delays in development work and communication.
	<i>Tool compatibility.</i> Are tools compatible across sites?	There are no compatibility issues between tools across sites.	Compatibility issues between tools create some collaboration barriers across sites.	Compatibility issues between tools create serious collaboration barriers across sites.
	<i>Configuration management.</i> How are configurations managed across sites?	There's appropriate configuration management across sites.	Configuration management is, with some exceptions, appropriate across sites.	There is limited configuration management across sites.

ond level focuses on developing risk assessments for the entire project based on the local estimates. This requires a colocated or mediated project meeting where participants uncover differences in perspectives and experiences across sites and negotiate how to prioritize overall distributed-team risks. Managers can distribute the resulting risk assessment data to the rest of the organization, allowing for risk management across subprojects and comparisons and learning among independent projects.

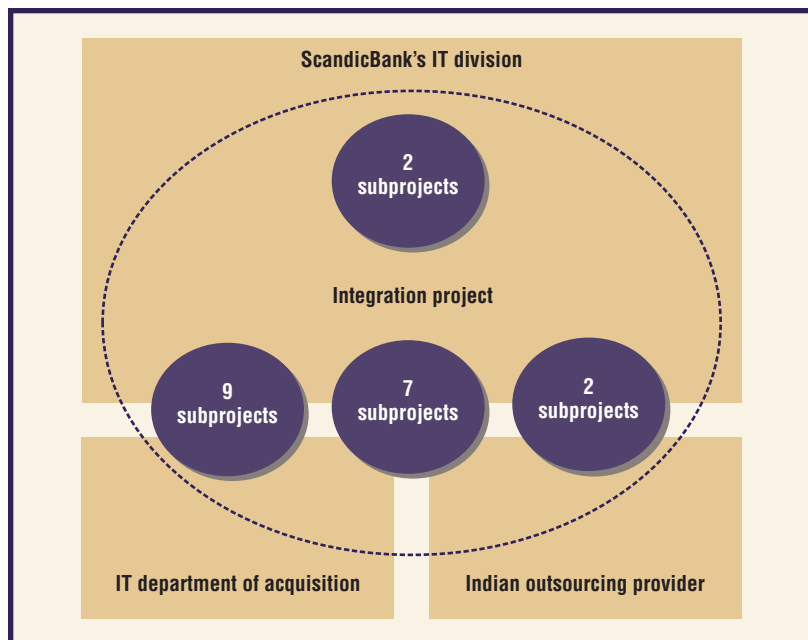
The process also helps distributed-team managers mitigate risks—CMMI's last specific goal for risk management.<sup>5</sup> Following the CMMI process, mitigating risks includes two specific practices: developing and implementing risk mitigation plans, steps 2 and 3 in Figure 1, respectively. Developing a risk mitigation plan is supported by the list of resolution techniques and guidelines for how to apply them to address specific risk areas (see Table 2).

During this step, participants can adopt resolution techniques from the list or develop novel resolution techniques to address distributed-team risks in their project. In the final process step, implementing risk mitigation plans, participants study project objectives and decide on practical approaches. To do so, they consider responsibilities, resources, deliverables, and milestones as key elements in implementation.<sup>7</sup>

### Process Illustration

We illustrate the risk management process with a software project from ScandicBank, a large financial company based in northern Europe. (ScandicBank is a pseudonym, but our discussion is based on data from a real-world distributed software project.)

ScandicBank has a long history of national mergers and is now expanding by acquiring



**Figure 2. ScandicBank's integration project. Rectangles are organizations, ovals are different types of subprojects spanning the organizations, and the large dotted oval indicates the entire integration project.**

companies in neighboring countries. Each acquisition requires a significant effort from ScandicBank's IT division. The strategy is to achieve economies of scale by implementing the bank's standard IT platform as quickly as possible in all new branches. The responsibility for the IT platform resides at ScandicBank's headquarters. However, some acquired companies have their own IT departments. After an acquisition, these are typically engaged in making the IT platform adhere to specific financial software system requirements in their respective countries.

ScandicBank's most recent acquisition is a company that's different from previous acquisitions. It's significantly larger, has a sophisticated IT platform, and is located in a country with a different language tradition from the dominant language within ScandicBank. Previous acquisitions were smaller, had an inferior IT platform, and involved a language tradition similar to ScandicBank.

The implementation of ScandicBank's standard IT platform is organized as an integration project (IP), as shown in Figure 2. The project consists of 20 subprojects, has more than 500 participants over its life cycle, and has a strict one-year deadline. The project participants are located in the acquired company's IT department and at four different sites of ScandicBank's IT division. Furthermore, the IP requires an unusually large number of IT professionals, so ScandicBank has engaged an Indian software outsourcing provider. Seven of the 20 subprojects have team members distributed across all three organizations, as illustrated in Figure 2; 11 subprojects are distributed

across ScandicBank's IT department and one of the two external entities; and only two subprojects aren't distributed.

## Identifying and Analyzing Risks

Identifying and analyzing risks is a nontrivial task in distributed teams. There are many types of risks and the knowledge to uncover them is typically distributed across team members and sites. Table 1 supports this task. The eight risk areas and related risks factors are defined by analytical questions and evaluation criteria related to the qualitative indicators of low, medium, and high.

Our approach takes into account the difficulties of communicating and sharing knowledge across distributed teams. First participants from each site individually use Table 1 to identify and analyze risks. Next the risk management participants discuss the local assessments at joint meetings across sites to arrive at an overall risk assessment and prioritization of risks. In large projects consisting of multiple subprojects, each subproject assessment would become the basis for a risk management meeting between subproject representatives.

Risk management participants apply Table 1 as follows to identify and analyze distributed-team risks. For each risk factor, the participants assess the probability of an unsatisfactory outcome  $P(UO)$  and the loss to the parties affected if the outcome is unsatisfactory  $L(UO)$ .<sup>7</sup> These assessments can be made on a scale with numeric values from 0 to 8, categorized into low (0–2), medium (3–5), and high (6–8). The qualitative indicators of low, medium, and high risk in Table 1 support the probability assessment.

Next, for each risk factor, the Web-based tool calculates the risk exposure (RE) based on the equation  $RE = P(UO) \times L(UO)$ .<sup>7</sup> The average RE for the three risk factors constitutes the risk area's RE value. On the basis of these values, the participants derive a prioritized list of the eight significant risk areas.

In ScandicBank's IT division, management gives high attention to the challenges related to the geographical distribution of software teams. Limited experience with distributed teams and the strategic importance of the company's most recent acquisition prompt management to adopt the risk management process. Development support makes the Web-based tool<sup>5</sup> available in the company's software methodology portfolio and includes the process in the IT division's process library. The IP manager initiates the process early during the requirements phase. Each subproject manager engages team members from the involved sites to



complete a local risk assessment according to Table 1 in preparation for a joint risk management meeting. At this point, the IP manager decides to repeat the risk management process at frequent intervals throughout the project's life cycle.

Several subprojects are in the fortunate position of having their first risk management meetings face-to-face, because colocated collaboration is emphasized for a few weeks during the requirements phase. So the IP participants predominantly carry out multinational requirements engineering in a colocated setting. This early stage colocation is feasible because the team has only a few members during the requirements phase (100), compared to later in the project (up to 500). Team members present and discuss local assessments of each risk factor using the Web-based tool and a projector.

Some subprojects can't meet face-to-face. They conduct risk management meetings using teleconferencing and desktop sharing of the results from the Web-based tool. In the beginning, participants are reluctant to comment on each others' risk assessments. In an effort to kick-start the discussion, one project manager points out the details of her risk assessment and volunteers to explain the grounds on which they were developed. To create an open and safe communication climate,<sup>3</sup> she then asks one of her more experienced and outgoing colleagues, who's not afraid to disagree with her, to elaborate on his assessment. Managers of distributed teams can undertake similar initiatives to overcome differences between high-context culture (India) and low-context culture (northern Europe) team members.<sup>14</sup>

With all subproject risk assessments in hand, the IP manager calls for a risk management meeting with all subproject managers. The procedure for this meeting is similar to that of the subprojects. However, participants compare and contrast the assessments of each subproject instead of the local assessments from each site. During the requirements phase in the first meeting, the project managers identify cultural distribution as the most significant risk area across subprojects. Also, it becomes clear that some subprojects have low assessments of all risk areas. These subprojects are primarily located at a single site within the IT division of ScandicBank with only a few team members at the IT department of the acquired company. As a consequence, the IP manager decides to include only six of the 20 subprojects in future risk management.

At later IP stages, the project managers evaluate task distribution as the most significant risk area. Over the project's life cycle, task distribution

and cultural distribution frequently have high-risk-exposure assessments whereas communication infrastructure and geographical distribution frequently have low-risk-exposure assessments.

### Developing Risk Mitigation Plans

Awareness of high-priority risk areas is an important first step in addressing them. However, it isn't sufficient. Effective risk management is based on comprehensive risk mitigation plans.

A variety of resolution techniques is available for developing risk mitigation plans. Table 2 associates techniques to different risk areas. In some situations, the proposed techniques oppose each other—for example, “Standardize and train in methods across sites,” on one hand, and “Handle differences in methods between sites,” on the other hand. The challenge is therefore to select a portfolio of coherent techniques that effectively address the risks at hand.

Instead of adopting the generic resolution techniques we suggest, users of the process can develop novel or company-specific techniques. The participants should develop risk mitigation plans at the joint risk management meetings and base them on the overall risk assessments for the project.

The IP adopts resolution techniques at both the overall project and subproject levels. For example, in a subproject with cultural distribution as a prioritized risk area, the participants choose the resolution technique “improve capability to manage cultural differences.” The Web-based tool provides detailed resolution suggestions as follows:<sup>5</sup>

- Establish courses in cultural diversity during the startup phase of the project. If team members are stationed at remote sites, the cultural training should take place before departure.
- Focus on creating understanding and acceptance of differences—for example, by letting each team member make a presentation on their individual culture, values, and expectations.
- Promote understanding and acceptance rather than seeking to streamline the project organization.
- Focus on the strengths that diversity offers rather than weaknesses.
- Acknowledge and discuss cultural differences in a respectful and civilized manner, and keep in mind that there are limits to cultural adaptation.
- Adjust management style according to culture—for example, team members' preferences for well-defined tasks versus preferences for loosely defined tasks and self-management.

**The challenge is to select a portfolio of coherent techniques that effectively address the risks at hand.**

**Table 2****Developing risk mitigation plans**

Risk areas/resolution techniques	Task distribution	Knowledge management	Geographical distribution	Collaboration structure	Cultural distribution	Stakeholder relations	Communication infrastructure	Technology setup
<b>Planning</b>								
Acquire complementary skills	X		X	X	X	X	X	X
Adjust meetings to distributed context	X	X	X				X	X
Divide tasks systematically between sites	X	X		X				
Reduce coupling between sites	X		X	X				
Create shared collaboration platform		X	X	X	X	X		X
Establish shared goals	X	X	X	X		X		
Establish communication norms		X	X		X	X	X	X
Define roles and responsibilities			X	X	X	X		
Reduce time-zone differences			X					
<b>Control</b>								
Focus on deliverables		X	X					X
Establish task coordination between sites	X			X				
Maintain site autonomy	X		X	X		X	X	
Establish shared control mechanisms	X	X	X	X		X		
Establish temporal coordination mechanisms	X	X	X	X				X
Maintain project organization overview	X	X	X	X			X	X
Maintain task overview within and across sites	X	X	X				X	X
Monitor and improve communication		X	X			X		X
Maintain a supportive environment	X		X		X	X		X
Analyze and manage errors	X	X						

Not all resolution suggestions are practically or financially feasible for the subproject. However, specific resolution suggestions spur debate and more specific ideas about how to address cultural distribution. The second resolution suggestion inspires a lunch meeting where one team member from each of the three countries makes a short presentation of their corporate and national culture. The participants discuss the strengths their cultural diversity offers and personal preferences regarding well-defined versus loosely defined tasks.

The subproject managers also discuss resolution techniques for cultural distribution at a risk management meeting for the IP at large. They discuss which resolution techniques to initiate across subprojects. They agree to mitigate risks primarily at this level by “developing liaisons between sites” (see Table 2). Each subproject with more than 10 team members will have liaisons at least at one ScandicBank IT division site, while subprojects with more than 25 team members will have liaisons at multiple sites.



**Table 2 cont'd**

**Developing risk mitigation plans**

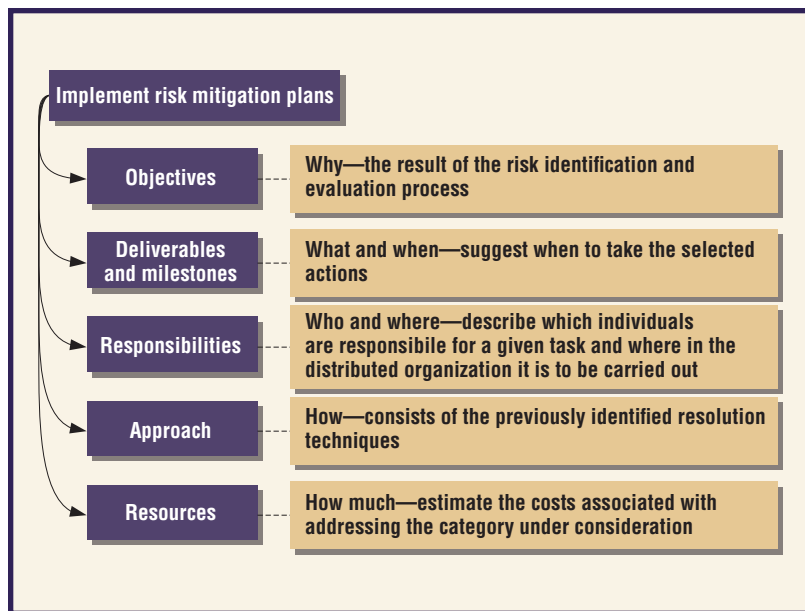
Risk areas/resolution techniques	Task distribution	Knowledge management	Geographical distribution	Collaboration structure	Cultural distribution	Stakeholder relations	Communication infrastructure	Technology setup
<b>Social integration</b>								
Improve capability to manage cultural differences		X	X		X			
Improve distributed collaboration skills			X	X		X	X	
Improve language skills					X			X
Emphasize early teambuilding activities			X			X	X	X
Promote humor and openness			X		X	X		
Use mentors to integrate new members	X	X				X	X	
Use face-to-face meetings appropriately	X	X	X	X		X	X	
Develop liaisons between sites	X	X	X		X	X	X	
Adopt shared reward systems				X	X	X		
<b>Technical integration</b>								
Increase technical compatibility between sites		X	X				X	X
Standardize and train in methods across sites	X	X		X	X			X
Adopt appropriate communication technologies	X	X	X		X	X	X	X
Improve collaboration and communication technology skills		X	X	X		X	X	X
Improve development technology skills		X						X
Handle differences in methods between sites		X		X				
Combine waterfall model and prototyping	X			X				

The subproject managers also discuss task distribution at a later risk management meeting. They agree to mitigate risks primarily through the “standardize and train in methods across sites” technique (see Table 2). Several subproject managers argue that team members outside the ScandicBank IT division lack knowledge of the development method, hindering effective task distribution among sites. The managers agree to organize training at the Indian site and the acquisition’s IT department.

### Implementing Risk Mitigation Plans

In risk management, it’s essential to reach conclu-

sions that lead to actions. The final step of our process is therefore to develop implementation plans for each prioritized risk area (see Figure 3). These plans lay out activities to bring each risk area under control. The plans address five basic elements of risk mitigation:<sup>7</sup> the *objectives* (why) are identified through the risk assessment; the *deliverables* and *milestones* (what and when) suggest when the team should take action; the *responsibilities* (who and where) describe which individuals are responsible for a given action and where they are to carry it out within the distributed organization; the *approach* (how) consists of the identified resolution



**Figure 3. Implementing risk mitigation plans by addressing the five elements of risk mitigation. The rightmost rectangles elaborate the question to consider for each element along with an explanation of how it relates to the process.**

techniques; and the *resources* (how much) estimate the costs associated with addressing the risk area. The project manager should then integrate the mitigation plans into the project's overall risk management plan.

In accordance with Figure 1, distributed projects should repeat the risk management process throughout the project life cycle as risk profiles change.<sup>6–8</sup> Distributed teams should therefore decide how often to revisit the risk management process and make sure that each activation is properly documented and reviewed in subsequent activations.

In the IP, the risk management participants detail the five elements of risk mitigation by the end of the joint risk management meetings. For example, in the subproject improving capabilities for managing cultural differences, the team implements the plan. The objective is to address cultural distribution because several team members expressed insecurity regarding how to contribute to the new distributed organization. The deliverables and milestones in relation to cultural distribution risks are the cultural presentation meetings scheduled at specific dates. Concerning responsibilities, the participants make notes on who should make cultural background presentations in each case. Adding to the approach, the participants make notes on what specific topics interest them. Finally, the participants estimate that the initiative represents a monthly two-hour resource load for each team member.

Two months later, when the risk management participants revisit the cultural distribution risk area, risk exposures have dropped from high to

medium. Hence, the initiatives have reduced culturally related misunderstandings and eased collaborations among team members.

The risk management meeting for the overall IP also addresses the five elements to implement more off-site training in ScandicBank's development method. The objective is to address task distribution because participants complain about task equivocality, particularly in regard to unclear testing and documentation responsibilities across sites. The deliverable is an extension of ScandicBank's method training program to be designed in three days and delivered in two weeks. A participant from development support and a subproject manager agree to take responsibility for the training initiative. In discussing the approach, several subproject managers request extended testing and documentation training. The participating managers estimate that these activities represent sizable resources, primarily covered by company-wide human resource efforts and thus not part of the IP budget. The participants estimate that the time invested by team members will give significant productivity payoffs for the remainder of the project.

When the risk management participants revisit the task distribution risk area two months later, risk exposure assessments are lower. The participants still perceive task equivocality as challenging. Therefore, in addition to the training initiative, the IP manager increases colocation of team members. While expensive, this additional initiative, which can be seen as an extreme adaptation of "develop liaisons between sites," proves successful in alleviating not only task distribution risks but also cultural distribution risks.

**G**eneric processes leave room for experimentation and suggestions for modifications.<sup>8</sup> In tailoring the process for managing distributed-team risks to match the preferences of your project or organization, you should therefore consider these guidelines:

- *Keep it simple.* Managing distributed teams has many challenges. It's important to establish a frequency of risk management that's appropriate for the organization and project. Participants shouldn't see the process as an unrewarding administrative burden. In some cases, the increased awareness resulting from risk management is more valuable than the resulting plans and initiatives.
- *Balance participation.* Distributed teams vary in size and complexity. In some cases, you only

want to involve a few participants from each site. In other cases, you might find it useful to involve all team members. Regardless of the number of participants, establishing an open and safe communication climate is vital for efficient risk management.

- **Adapt taxonomies.** We've designed our process for a variety of preferences. Some elements of the architecture might not fit your project or organization. For example, you might want to include additional resolution techniques—a specific consultant, a particular course, or available technologies—when developing risk mitigation plans.
- **Integrate plans.** Managing distributed-team risks is only one aspect of risk management. Moreover, risk management is only one of many key disciplines in project management. For each project, you need to integrate the process into project management at large. Appropriate software systems can be a significant help in such integrations.
- **Attract capabilities.** Practicing the process will clarify the specific capabilities needed to effectively manage distributed teams. As you move forward through the project life cycle, or as you engage in new distributed teams, you should attract complementary capabilities to proactively reduce the probability and impact of distributed-team risks.

Talented managers make projects work regardless of colocation or distribution. Our risk management process can help managers to systematically assess and control the risks they face in specific distributed projects. By utilizing the extensive literature on distributed teams<sup>5</sup> and established practices for developing software,<sup>6</sup> we hope the process can help managers avoid the failures and repeat the successes of past distributed teams. ☞

## References

1. J.D. Herbsleb and D. Moitra, "Global Software Development," *IEEE Software*, vol. 18, no. 2, 2001, pp. 16–20.
2. S. Sakthivel, "Managing Risks in Offshore Systems Development," *Comm. ACM*, vol. 50, no. 4, 2007, pp. 69–75.
3. C.B. Gibson and J.L. Gibbs, "Unpacking the Concept of Virtuality: The Effects of Geographic Dispersion, Electronic Dependence, Dynamic Structure, and National Diversity on Team Innovation," *Administrative Science Quarterly*, vol. 51, no. 3, 2006, pp. 451–495.

## About the Authors



**John Stouby Persson** is a postdoctoral student in Aalborg University's Department of Computer Science. His research interests include information systems development, IT project management, and virtual organizations. Persson received his master's degree in informatics from Aalborg University. He's a member of the Association for Information Systems. Contact him at [john@cs.aau.dk](mailto:john@cs.aau.dk).

**Lars Mathiassen** is a Georgia Research Alliance Eminent Scholar and professor in Georgia State University's Department of Computer Information Systems and cofounder of its Center for Process Innovation. His research interests include information systems and software engineering, with an emphasis on process innovation. Mathiassen has a PhD in informatics from Oslo University and a Dr. Techn. in software engineering from Aalborg University. He coauthored *Computers in Context* (Blackwell, 1993), *Object Oriented Analysis & Design* (Marko Publishing, 2000), and *Improving Software Organizations* (Addison-Wesley, 2002). He's a member of the IEEE, the ACM, and the Association for Information Systems. Contact him at [lmathiassen@ceprn.edu](mailto:lmathiassen@ceprn.edu).



4. D.C. Gumm, "Distribution Dimensions in Software Development Projects: A Taxonomy," *IEEE Software*, vol. 23, no. 5, 2006, pp. 45–51.
5. J.S. Persson et al., "Managing Risks in Distributed Software Projects: An Integrative Framework," *IEEE Trans. Eng. Management*, vol. 56, no. 3, 2009, pp. 508–532.
6. CMMI Product Team, *CMMI for Development*, v. 1.2, tech. report CMU/SEI-2006-TR-008, Carnegie Mellon Software Eng. Inst., 2006.
7. B.W. Boehm, "Software Risk Management—Principles and Practices," *IEEE Software*, vol. 8, no. 1, 1991, pp. 32–41.
8. M.K. Kulpa and K.A. Johnson, *Interpreting the CMMI: A Process Improvement Approach*, CRC Press, 2003.
9. A. Powell, G. Piccoli, and B. Ives, "Virtual Teams: A Review of Current Literature and Directions for Future Research," *The Data Base for Advances in Information Systems*, vol. 35, no. 1, 2004, pp. 6–36.
10. J.M. Bhat, M. Gupta, and S.N. Murthy, "Overcoming Requirements Engineering Challenges: Lessons from Offshore Outsourcing," *IEEE Software*, vol. 23, no. 5, 2006, pp. 38–44.
11. D. Damian, "Stakeholders in Global Requirements Engineering: Lessons Learned from Practice," *IEEE Software*, vol. 24, no. 2, 2007, pp. 21–27.
12. F.W. McFarlan, "Portfolio Approach to Information Systems," *Harvard Business Rev.*, vol. 59, no. 5, 1981, pp. 142–150.
13. J.H. Iversen, L. Mathiassen, and P.A. Nielsen, "Managing Risk in Software Process Improvement: An Action Research Approach," *MIS Quarterly*, vol. 28, no. 3, 2004, pp. 395–433.
14. E.T. Hall, *Beyond Culture*, Anchor Press, 1977.
15. S. Sakthivel, "Virtual Workgroups in Offshore Systems Development," *Information and Software Technology*, vol. 47, no. 5, 2005, pp. 305–318.



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.